



DEPARTMENT OF THE ARMY

HEADQUARTERS UNITED STATES ARMY TRAINING AND DOCTRINE COMMAND
FORT MONROE, VIRGINIA 23651-5000

REPLY TO
ATTENTION OF

ATIM-I (380-19)

22 MAY 00

MEMORANDUM FOR

Commander, U.S. Army Recruiting Command, 1307 3rd Avenue,
Fort Knox, KY 40121-2726
Director, U.S. Army Nuclear and Chemical Agency, 7510 Heller
Loop, STE 101, Springfield, VA 22150-3198
Commanders, TRADOC Installations
Chiefs of General and Special Staff Offices, HQ TRADOC

SUBJECT: Security of File Transfer Protocol (FTP) Services

1. Reference AR 380-19, Information Systems Security (ISS) Program, 27 Feb 98.
2. This memorandum provides procedures and interim TRADOC policy for minimizing ISS risks associated with FTP servers.
3. The use of FTP services poses known ISS risks. Without adequate safeguards, hackers and intruders can access FTP servers, which creates the opportunity for unauthorized disclosure of information, remote attacks, execution of arbitrary commands with root privileges, and system/network compromises.
4. FTP security deficiencies:
 - a. By default, passwords are transmitted in plain text, enabling electronic eavesdropping and capture of passwords.
 - b. FTP sessions are not encrypted and offer no secure transmissions.
 - c. The ability to restrict access to FTP sites varies with operating systems, leaving FTP sites vulnerable to unauthorized users.

ATIM-I

SUBJECT: Security of File Transfer Protocol (FTP) Services

5. Implementation of a restricted access FTP server is discouraged because FTP services do not truly restrict access and leads to a false sense of security. Restricted access FTP servers provide only limited security based on IP address filtering. Passwords transferred across the network-using FTP are sent in plain text and are easily intercepted. Search engines have the ability to index restricted access FTP and make files accessible if permissions are not properly configured.

6. To mitigate the ISS risks associated with FTP services, implement the following procedures immediately:

a. Review the need, purpose and target users for FTP services. If not essential, eliminate FTP services. More secure methods to transfer data files include:

(1) Web pages hyper-linked to files.

(2) Use of network shares/files permissions (i.e., intranet folders/directories).

(3) Email attachments (for small target audiences and small file sizes).

b. If FTP services are essential, use the enclosed FTP security checklists to establish an FTP server. Additional technical assistance can be obtained through the Regional Computer Emergency Response Team (RCERT)-CONUS, DSN: 879-2482/COM: (602) 538-2482.

7. The above procedures are in addition to AR 380-19 policy and the command and control protect (C2P) procedures published for data networks and servers.

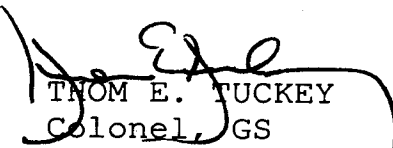
ATIM-I

SUBJECT: Security of File Transfer Protocol (FTP) Services

8. Point of contact is MAJ Steve Rehn, DSN: 680-3829, COM:
(757) 727-3829, E-mail: steven.rehn@monroe.army.mil.

FOR THE COMMANDER:

Encl
as


THOM E. TUCKEY
Colonel, GS
Deputy Chief of Staff
For Information Management